ソリューション概要

FireEye

脅威インテリジェンスのユースケース・シリーズ

脆弱性管理アナリスト

脆弱性管理アナリストが抱える課題

脆弱性の情報収集や優先度の判断を担当するアナリストや管理者は、次のようにさまざまな課題に直面しています。

- ソフトウェア・ベンダーやセキュリティ・コンサルタント、さらにはハッカーやサイバー犯罪者などにより、新たな脆弱性の存在が次々と明らかにされる。
- 脆弱性データベースに登録されている脆弱性の多くはリスク・スコアが高く（たとえば、National Vulnerability Databaseに登録されている脆弱性の41%は、CVSSスコアが7～8、8～9、9～10）、特に優先度の高い脆弱性を見極めるのは非常に困難。
- 1か月あたり数百件単位で明らかになる脆弱性のうち、特定の業種や地域、組織への影響が大きい脆弱性を見分けるための情報がほとんどない。
- 脆弱性の悪用を可能にするエクスプロイトの有無や、高度な攻撃で使用される可能性の高いエクスプロイトの判断が困難。

パッチ管理においては、公開されたすべてのパッチを直ちに適用できる状況が理想です。…しかし、この理想を実現するのは容易なことではありません。人手が限られている多くの組織では、優先度の高いパッチを見極め、そのパッチを先に適用する必要があります。

— NIST Special Publication 800-40 Revision 3

脆弱性管理アナリスト

ほとんどのIT部門には、脆弱性に関する情報を収集して優先度を判断し、対応計画の策定を支援するアナリストが存在するはずです。所属するチームは、セキュリティ・オペレーション、セキュリティ・エンジニアリング、コンプライアンス/リスク管理など、組織によってさまざまですが、主に次のような作業を担当しています。

- 組織で運用しているサーバー、デバイス、エンドポイント、アプリケーションを確認し、その脆弱性を把握する。
- 新たに見つかった脆弱性のうち、組織にとって深刻なリスクをもたらす脆弱性と優先度の低い脆弱性を見極める。その際には、脆弱性の重大度、組織で運用しているシステムやアプリケーション、導入済みのセキュリティ対策、その脆弱性がすでに悪用されているかどうかなどの要素を考慮する。
- 適切な緩和策の策定を支援する。
- 監査担当者、リスク・マネージャ、その他のIT担当者に、短時間では対応できない脆弱性のリスクについて説明する。

表1：ユースケース – 脆弱性管理アナリスト

ユースケース	主な目標	必要なインテリジェンス
脆弱性の解析	• タイプ、対象、想定される標的別に脆弱性を分類する • 高度な攻撃における脆弱性の悪用シナリオを把握する	• 脆弱性、攻撃グループ、攻撃手法、想定される標的に関するインテリジェンス・ナレッジベース • 特定の業種や組織に特化した脅威解析レポート
脆弱性の優先度の判定	次に当てはまる脆弱性を特定する • 組織で運用しているシステムやソフトウェアに影響する • 既存のセキュリティ対策では緩和できない • 攻撃者による悪用が確認されている	• インテリジェンス・ナレッジベース • 現在使用されている攻撃手法とアンダーグラウンドなWebサイトで提供されているエクスプロイト・キットに関する調査結果
緩和策の特定	• 脆弱性のパッチを入手する • パッチに替わる適切な緩和策を見つける	• 緩和策を推奨するインテリジェンス・ナレッジベース
リスク・マネージャやシステム管理者とのコミュニケーション	• 対策完了まで監視する必要があるハイリスクなシステムを特定する	• インテリジェンス・ナレッジベース • 特定の業種や組織に特化した脅威解析レポート

脆弱性管理アナリストによるサイバー脅威インテリジェンスの活用

最近では、深刻な脆弱性の見極め、適切な緩和策の策定、マネージャやその他のIT担当者とのリスク・コミュニケーションに、サイバー脅威インテリジェンスを活用する動きが脆弱性管理アナリストの間で広がっています。

サイバー脅威インテリジェンスがもたらすメリット

1. 脆弱性の関連性と重大度を把握する

サイバー脅威インテリジェンスを利用すると、特定の脆弱性を悪用する攻撃グループを特定し、その戦術、技術、手順（TTP）、標的を把握できます。脆弱性管理アナリストは、この情報に基づき、組織で運用しているシステムやソフトウェアに影響する脆弱性、特定の業種や地域を標的とする攻撃者に悪用される可能性が高い脆弱性を見極めることができます。

2. エクスプロイト/エクスプロイト・キットに関する情報を入手する

サイバー脅威インテリジェンス・ベンダーの研究者は、エクスプロイト/エクスプロイト・キットに関する情報を追跡しています。エクスプロイト/エクスプロイト・キットの売買や情報交換は、主にハッカーやサイバー犯罪者が利用する「ダークWeb」で行われています。効果的なエクスプロイト・キットが存在する脆弱性は、近い将来に悪用される可能性が非常に高くなります。脆弱性管理アナリストは、この情報を利用して、即時のパッチ適用や緩和策の実施が必要な脆弱性と、緊急性の低い脆弱性を見極めることができます。

3. 緩和策を実施する

サイバー脅威インテリジェンス・ナレッジベースには、特定の脆弱性を解決するパッチについての情報に加えて、パッチが提供されていない場合や適用に時間を要する場合に実施できる緩和策についての情報も含まれています。緩和策の例としては、従来型のファイアウォールやアプリケーション・ファイアウォール、侵入防御システムのルールの作成、脆弱性のあるシステムの設定変更、アクセス・ポリシーやパスワード・ポリシーの強化・徹底、脆弱性を抱えたシステムやアプリケーションの監視強化などがあります。

4. ビジネス・リスクを明確にする

サイバー脅威インテリジェンスは、高度な攻撃における脆弱性の悪用シナリオについての情報を提供するほか、ローカルのアナリストなどが提供するビジネス・コンテキストを組み合わせることで、組織のビジネス・リスクの評価にも役立てることができます。アナリストや管理者は、これらの情報をもとに、脆弱性がビジネスにもたらす影響や、パッチの適用や緩和策の実施が終わるまで監視を強化する必要があるシステムをIT部門やビジネス部門の管理職に伝えることができます。

まとめ

脆弱性管理アナリストがサイバー脅威インテリジェンスを利用すれば、次のようなメリットが実現します。

- 特定の脆弱性が、誰にどのようにして悪用される可能性があるかを理解する。
- 特定の業種や組織が直面する現実の脅威、有効なセキュリティ対策の有無、エクスプロイトの有無に基づいて脆弱性の優先度を的確に判断し、ビジネス・リスクを軽減する。
- 適切な緩和策を把握、実施する。
- 監査担当者、リスク・マネージャ、その他のIT担当者に、脆弱性がもたらすリスクをビジネスの観点で説明する。

FireEye製品の詳細については、次のWebページをご覧ください。
www.FireEye.jp

ファイア・アイ株式会社 | 〒101-0054 東京都千代田区神田錦町3-22 テラススクエア8階 | 03−4577−4401 | Japan@fireeye.com | www.fireeye.jp
FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.FireEye.com